QUALYSEC
BEYOND CYBERSECURITY

2023

AUG 5TH WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

SapphireStealer: A .NET Malware Capable of Stealing Sensitive Data from Computers

SapphireStealer is an open-source information stealer that may be utilized for obtaining sensitive information, such as corporate credentials, which are frequently sold to other threat actors who utilize the access for further attacks, such as espionage or ransomware/extortion schemes.

On December 25, 2022, the codebase for SapphireStealer was made available on GitHub. According to Cisco Talos researchers, beginning in mid-January 2023, newly created SapphireStealer versions started appearing in public malware repositories.

Presently, many threat actors are using this malware codebase. This danger already exists in many forms, and threat actors constantly enhance its potency and efficacy.

The Working of SapphireStealer

Information-stealing malware dubbed SapphireStealer was created in .NET. It provides simple yet efficient functionality capable of stealing private data from compromised systems, such as:

Host information , Screenshots, Cached browser credentials,

Files stored on the system that match a predefined list of file extensions.

Source : https://cybersecuritynews.com/sapphirestealer-net-malware/

North Korea's Hacker Group Deploys Malicious Version of Python Package in PyPI Repository

ReversingLabs spotted "VMConnect" in early August, a malicious supply chain campaign with two dozen rogue Python packages on PyPI.

It's been observed that these packages mimicked the following known open-source Python tools:-

- vConnector
- eth-tester
- Databases

Cybersecurity researchers at ReversingLabs recently identified that a North Korean hacker group is actively deploying malicious versions of Python Packages in the PyPI repository.

The security analysts analyzed all the malicious packages, and after successfully decrypting the malicious packages, they linked their roots to Labyrinth Chollima, a branch of the renowned North Korean state-sponsored group Lazarus.

Recent years witnessed malicious actors imitating open-source packages, using tactics like typosquatting to trick busy developers into installing malware.

Source : https://cybersecuritynews.com/malicious-pypi-repository/

Junos OS Flaw Allows a Network-based Attacker to Launch DoS Attack

Junos OS and Junos OS Evolved have been found to be vulnerable to a DoS (Denial of Service) condition, which an unauthenticated, network-based attacker can exploit.
Juniper Networks has addressed this vulnerability on their security advisory along with certain workarounds.

Junos OS evolved, and Junos OS was built on Linux Kernel and FreeBSD kernel, respectively, that uses a BGP session which enables the exchange of routing between the internet and the large networks of systems.
At the end of August, a pre-auth RCE was reported, and additional details about the proof of concept have been published.
However, Juniper Networks has released patches for fixing this vulnerability.

CVE-2023-4481: DoS (Denial of Service) in Routing Protocol Daemon
The BGP UPDATE messages are received over an established BGP session which can be terminated with an UPDATE message error. This UPDATE message can be specially crafted by a threat actor and can go through unaffected systems and intermediate BGP speakers.

Source : https://cybersecuritynews.com/junos-os-flaw-dos-attack/

AI Coding Platform Sourcegraph Breached Via Leaked Admin Access Token

On August 30, 2023, a malicious actor gained unauthorized access to specific Sourcegraph(.)com data through a leaked admin access token. Sourcegraph is a code AI platform that makes it easy to read, write, and fix code–even in big, complex code bases.

In a recent notice, Sourcegraph confirmed that a security breach occurred, but only limited data was accessed:

– For the Paid Customers: The attacker accessed the license key recipient's name and email address. A subset of Sourcegraph license keys may have been accessed; affected customers will be contacted to rotate their license keys.

– For the Community Users: Only Sourcegraph account email addresses were accessed, and no further action is required from these users.

"No other sensitive customer information such as private code, emails, passwords, or usernames was compromised," said Diego Comas, the Head of Security of Sourcegraph.

Substantial Increase in API usage

On August 30, 2023, Sourcegraph's security team detected a substantial increase in API usage on Sourcegraph.com, leading to an investigation.

Source : https://cybersecuritynews.com/ai-coding-platform-breached/

Hackers Abuse Windows Container Isolation Framework to Bypass Security Defences

Recently, cybersecurity researchers at Deep Instinct have asserted that hackers can exploit the Windows container isolation framework to bypass the security defenses and mechanisms of organizations.

Containers revolutionize the way applications are packaged and isolated, empowering them with their complete runtime environment enclosed within.

That's why the containers are crucial for resource efficiency and security. Besides this, Microsoft introduced Windows Container in Windows Server 2016, which offers the following two key distinct modes:-

- Process isolation mode
- Hyper-V isolation mode

Hackers Abuse Windows Container Isolation

Since Windows Server 2003, job objects group processes for unified management, as they control attributes like-

- CPU
- I/O
- Memory
- Network use

Source : https://cybersecuritynews.com/hackers-abuse-windows-container-isolation-framework/

Cisco Unified Communications Products Flaw Let Attackers Escalate Privileges

A recent discovery has highlighted a privilege escalation vulnerability within Cisco Unified Communications Products. This vulnerability was found during internal security testing.

Cisco Unified Communications Manager (CUCM) and Cisco Unified Communications Manager Session Management Edition (CUCM SME) have been found to contain a privilege escalation vulnerability.

This vulnerability, designated CVE-2023-20266, allows an authenticated attacker with administrative access to elevate their privileges and execute arbitrary code with root-level privileges.

This vulnerability is due to the application's failure to adequately limit the types of files utilized for upgrades.

A malicious actor could take advantage of this weakness by submitting a specially crafted upgrade file. If successfully exploited, this vulnerability could enable the attacker to gain higher-level privileges, potentially reaching root access.

Cisco Unified Communications Products Flaw

Privilege escalation vulnerabilities are particularly concerning as they grant unauthorized users elevated privileges, essentially granting them control over the affected system.

Source : https://cybersecuritynews.com/cisco-unified-communications-products-flaw/

Splunk IT Service Intelligence Injection Flaw Let Attacker Inject ANSI Codes in Log Files

Splunk has been reported with a Unauthenticated Log injection vulnerability in the Splunk IT Service Intelligence (ITSI) product. This vulnerability exists in Splunk ITSI versions prior to 4.13.3 or 4.15.3.

Splunk ITSI is an Artificial Intelligence Operations (AIOps) powered monitoring and analytics solution that provides users with visibility about the health of critical IT and business services and their infrastructure.

CVE(s):

CVE-2023-4571: Unauthenticated Log Injection in Splunk IT Service Intelligence (ITSI)

This vulnerability can be exploited by a threat actor by injecting an American National Standard Institute (ANSI) escape code inside the Splunk ITSI log files that can run malicious code in the vulnerable application if a vulnerable terminal application reads it.

However, this vulnerability requires user interactions to be performed. The user must read the malicious log file using a terminal application that translates the ANSI escape codes in the vulnerable terminal.

This vulnerability can be exploited by threat actors to perform malicious actions like copying the malicious file from Splunk ITSI and reading it on their local machine.

Source : https://cybersecuritynews.com/splunk-it-service-intelligence-flaw/

Critical Flaw in Zip Libraries Let Attackers Abuse ZIP archives

According to recent reports, a number of vulnerabilities have been discovered in widely used ZIP libraries of Swift and Flutter.

These packages are being utilized by numerous developers and applications, which significantly increases the potential attack surface.Developers use ZIP packages to create a bundle of libraries, components, resources, and other app files used for the application's functionality. A malicious ZIP package can severely impact the application and compromise its security.

Structure of a ZIP file

A ZIP file has four major parts that construct its structure. These parts have different functions, from the ZIP archive's file name to the central directory's access. The parts are,

- Local File Header – Contains essential information such as the file's name, compression method, size, and other attributes.
- Data Descriptor – Stores CRC 32 (Cyclic redundancy check 32) checksum of the uncompressed data, the compressed and uncompressed data.
- Central Directory File Header – Contains metadata of each file within the archive..

Source : https://cybersecuritynews.com/critical-flaw-zip-libraries/

Mozilla Firefox 117: 5 High-Severity Vulnerabilities Patched

With the release of Mozilla Firefox 117, 13 vulnerabilities are patched, including seven 'High Severity' flaws and four memory corruption flaws.

Mozilla said that IPC CanvasTranslator, IPC ColorPickerShownCallback, IPC FilePickerShownCallback, and JIT UpdateRegExpStatics components of the browser are all affected by these memory corruption issues, which might result in potentially exploitable crashes.

High-Severity Flaws Addressed

The high severity flaw tracked as CVE-2023-4573, Memory corruption in IPC CanvasTranslator, reported by Sonakkbi has been addressed.

When receiving rendering data through IPC, mStream may have been initialized and then destroyed, which could have resulted in a use-after-free and a crash that might have been exploited.

Memory corruption in IPC ColorPickerShownCallback tracked as CVE-2023-4574 has been fixed. The issue was reported by Sonakkbi.

A high-severity Memory corruption bug in IPC FilePickerShownCallback tracked as CVE-2023-4575 has been addressed. The issue was reported by Sonakkbi.

Source : https://cybersecuritynews.com/firefox-high-severity-vulnerabilities/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT